National ANPR Service Project

NAS Gateway Specification

Author:	Jon Linsdell
Date:	3rd April 2017
Version:	3.0
Status:	Issued

This and other National ANPR Service Project Documents are published on POLKA

Please register with the 'ANPR' community on POLKA
to view the latest material from the NAS Project.

Click on 'Documents' tab along the top - then access 'NAS Project' folder area on the left

Contact nas.project@homeoffice.gsi.gov.uk with questions or to find out more

Document History

Version	Date	Details of Changes included in Update	Author (s)
1.0	07/12/2015	Issued as version 1	M Griffiths
2.0	31/05/2016	Issued as version 2	M Griffiths
3.0	03/04/2017	Issued as version 3. Major update following programme re-launch.	J. Linsdell

Reference Documents

#	Document Title	Version and Issue Date
1.	National ANPR Standards for Policing (Parts1, 2 & 3)	NAS Version, April 2016
2.	NAS Management Server Test Plan	March 2017
3.	LPR Core REST API Document	Version 3.0
4.	LPR Core API XML Specification	Version 3.0
5.	NAS DRDD	Version 1.2

Abbreviations and Accronyms

ANPR	Automatic Number Plate Recognition
API	Application Programming Interface
BOF	Back Office Facility
GPS	Global Positioning System
GUID	Global Unique Identifier
NADC	National ANPR Data Centre
NAS	National ANPR Service
NASP	National ANPR Standards for Policing
NRD	Number Plate Reading Device
PNC	Police National Computer
PSN	Public Services Network
REST	Representational State Transfer
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VOI	Vehicle of Interest
VRM	Vehicle Registration Mark
XML	eXtensible Markup Language

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this document is to specify the requirements that must be met by a management server in order to fulfil the needs of the overall National ANPR Service (NAS). Law Enforcement Agencies (LEAs) may require additional functionality to be provided within a management server. This additional functionality is outside of the scope of NAS and must be in accordance with the National ANPR Standards for Policing (NASP), ref [1].

1.2 Approach

The requirements contained within this document have been developed using the NAS Detailed Requirement Definition Document (DRDD), ref [5], NASP, ref [1] and the LPR Core REST API Document, ref [3].

The document has been structured as follows:

- Section 2 provides an overview of the NAS solution and a description of the role of management servers
- Section 3 details the management server requirements. Each subsection contains a descriptive overview, aimed at providing context and a table containing the specific requirements.
- Section 4 provides additional guidance to support management server suppliers and LEAs develop their solutions. The contents of this section do not constitute formal requirements.

2. Solution Overview

This section provides a brief overview of the NAS solution and the management server concept.

2.1 NAS Solution Overview

NAS is being introduced to replace the existing national ANPR solution provided through LEA Back Office Facilities (BOFs) and the National ANPR Data Centre (NADC), with the aim of centralising the capability. This means that much of the functionality that currently resides in BOFs will migrate to NAS.

ANPR reads captured by Number Plate Reading Devices (NRDs) will be sent to NAS. NAS will provide the interface to the Police National Computer (PNC) to allow alerting against national Vehicle of Interest (VOI) lists. NAS will also be capable of ingesting externally managed VOI lists, such as those provided by the Drivers and Vehicle Licensing Agency and the Motor Insurers' Bureau, as well as those managed by LEAs locally. On a day-to-day basis, ANPR users will login to NAS through a web browser to access the system, manage alerts and perform complex searches.

Through an Application Programming Interface (API), the NAS application provides a mechanism for ANPR reads to be sent from local LEA systems and for the retrieval of specific data for onward communication to mobile units. On the LEA side of the interface, the coordination with NAS for sending and retrieving data will be undertaken by a management server. Figure 1 shows an overview of the NAS solution.

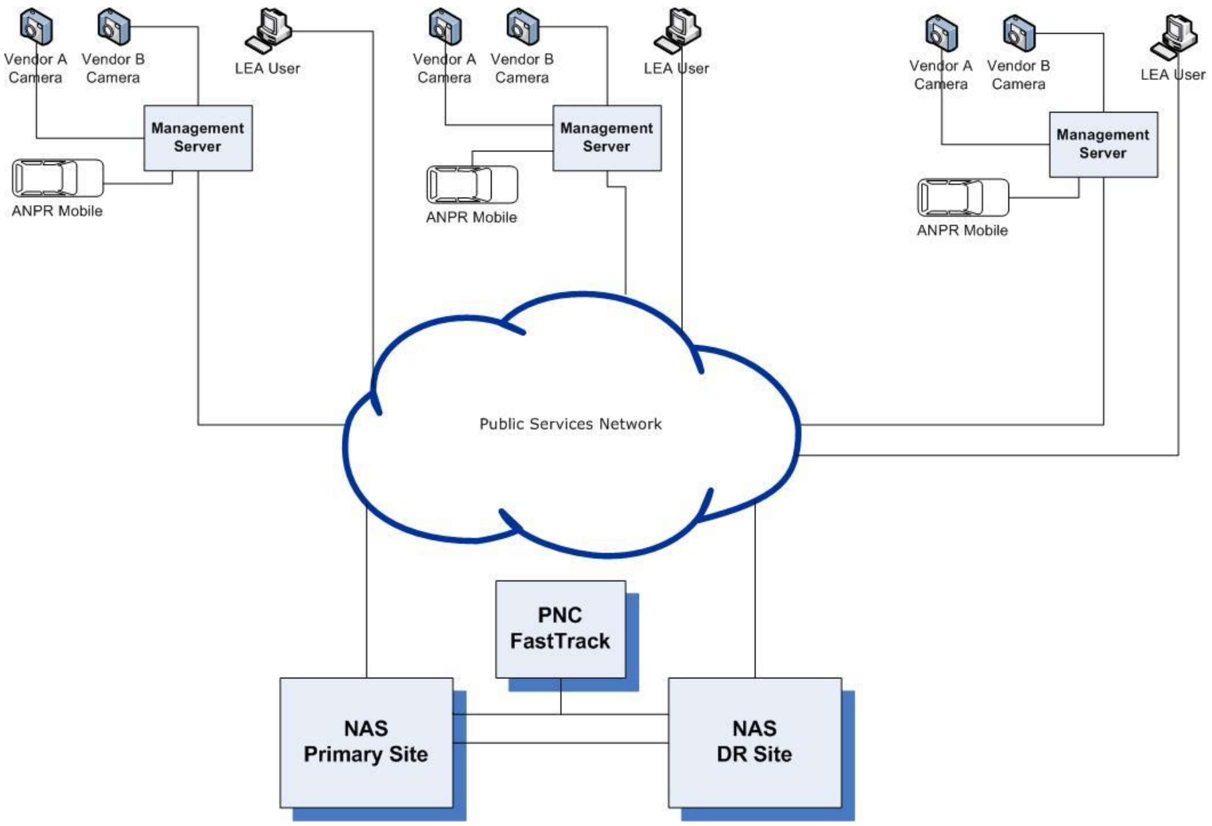


Figure 1: NAS Solution Overview

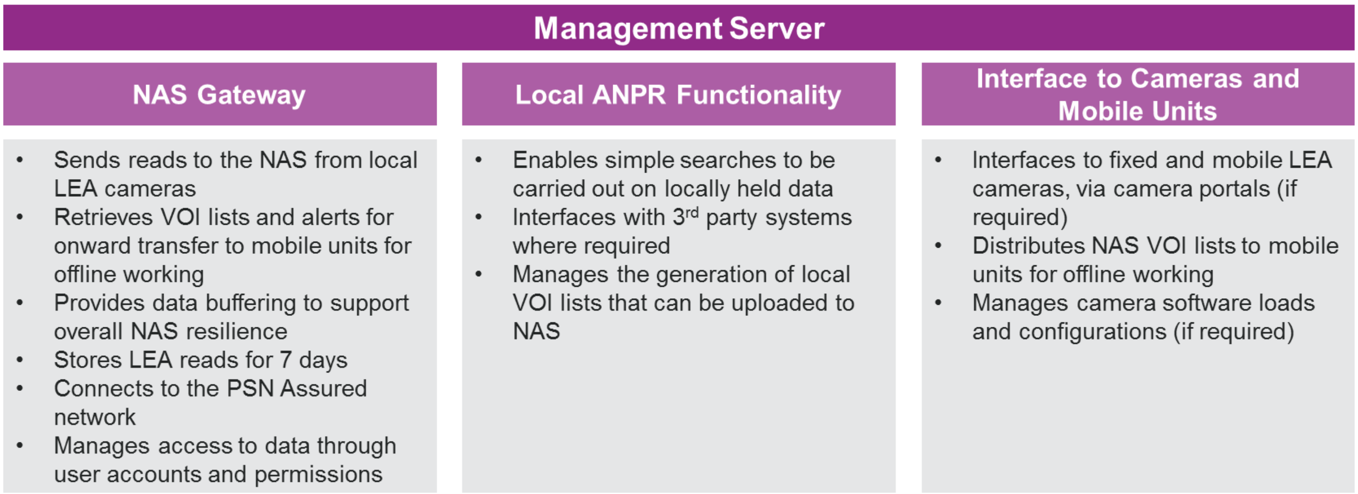
2.2 Management Server Overview

The role of a management server is to coordinate the delivery of ANPR reads to NAS and the retrieval of data from it. A management server will be able to connect to the existing NRD and mobile unit infrastructure for a LEA, receiving ANPR reads from the NRDs and providing data to mobile units for offline working. In this respect, the management servers will replace the BOFs that LEAs currently use. All other BOF functionality should be provided by the central NAS application.

Management servers have 3 components:

1. A gateway to NAS, providing the functions required to ensure that the NAS solution can deliver the output required. The functionality provided here should be consistent across management servers and change to this component of the management server will be driven by changes to the core NAS functionality.
2. Interface to cameras and mobile units. This element is dependent on the existing mobile units and NRD systems in place for each LEA; therefore must be tailored to each LEA. Changes to this component will be driven by changes to the LEA camera and mobile unit estate.
3. Local ANPR functionality. This element is entirely down to the working practices of the LEA. It may provide a level of local search capability for when connection to NAS is not available or interface to other systems.

Figure 2 provides an overview of the key functions of each of the management server components.



Management Server

NAS Gateway

- Sends reads to the NAS from local LEA cameras
- Retrieves VOI lists and alerts for onward transfer to mobile units for offline working
- Provides data buffering to support overall NAS resilience
- Stores LEA reads for 7 days
- Connects to the PSN Assured network
- Manages access to data through user accounts and permissions

Local ANPR Functionality

- Enables simple searches to be carried out on locally held data
- Interfaces with 3rd party systems where required
- Manages the generation of local VOI lists that can be uploaded to NAS

Interface to Cameras and Mobile Units

- Interfaces to fixed and mobile LEA cameras, via camera portals (if required)
- Distributes NAS VOI lists to mobile units for offline working
- Manages camera software loads and configurations (if required)

Figure 2: Management Server Components

The requirements contained within this document are only concerned with the NAS Gateway component of the management servers. Requirements for the other elements will need to be discussed and agreed with the LEAs.

3. NAS Gateway Requirements

The following subsections provide an overview of the required functionality for each functional area and the specific requirements to be met in the Management Server design to meet the needs of NAS. The description is intended to provide context to support the requirements. The requirements identified are those that will be tested during integration and connection testing as defined in the NAS Management Server Test Plan, ref [2].

3.1 Standards

All ANPR systems operated by LEAs in the UK and that connect to, or receive data from the NAS must adhere to the National ANPR Standards for Policing (NASP).

Reqt ID	Requirement
MS001	The Management Server shall operate in accordance with the National ANPR Standards for Policing

3.2 NRD Ingestion

The Management Server within a LEA will provide the mechanism for ANPR reads captured by local Number Plate Reading Devices (NRDs) to be sent to NAS. This is achieved by using an Application Programming Interface (API) developed by the NAS application supplier. Management Servers will need to ensure that the data provided to NAS meets the requirements specified in NASP and is assembled in a valid structure for the API. The Management Server will need to be able to connect to existing NRD infrastructure used by the LEAs.

The data will be accepted by NAS providing it contains a valid VRM and camera identifier. Where this is not the case, NAS will reject the data and provide an error message to the Management Server. When an error message is received, the Management Server will automatically retain the data and provide notification to the system administrators so that further action can be taken.

The Management Server must confirm that all reads have a valid camera identifier. Where a lookup of the camera identifier identifies either a duplicate Globally Unique Identifier (GUID) or no GUID, processing of that camera's ANPR reads will be suspended and the Management Server will notify an administrator. Read processing will resume on correction of the camera name or creation of the camera name in NAS. NAS will hold the master list of cameras. Management Server will maintain an up-to-date copy of the list locally for the purposes of lookup of GUIDs.

The Management Server must be capable of suspending ANPR reads from specific cameras from being passed on to NAS.

Reqt ID	Requirement
MS002	The Management Server shall ensure that only NASP compliant ANPR read data is sent to NAS
MS003	The Management Server shall capture and store reads, including images from NRDs, using the existing LEA NRD infrastructure.
MS004	The Management Server shall assemble valid XML messages for the submission of ANPR read data to NAS in accordance with the NAS XML schema
MS005	The Management Server shall automatically retain data upon a receipt of an error message from NAS
MS006	The Management Server shall provide a visual notification that data is not valid and has been stored
MS007	The Management Server shall ensure that ANPR read data sent to NAS has a valid camera identifier.
MS008	The Management Server shall allow ANPR read data to be suspended or enabled at camera-level, preventing reads from being sent to NAS
MS009	The Management Server shall allow GPS coordinates for NRDs to be entered where the NRD does not provide them as part of the read data.

3.3 Performance and Capacity

NASP requires that NAS provides real-time matching to Vehicle Of Interest (VOI) lists. This covers the response time from a VRM being captured to the hit notification response being delivered to a specific operator.

For static, moveable, dual lane and CCTV ANPR Integrated systems the overall response time required is 4 seconds, with 2 seconds allocated to NAS to process the read and generate the hit notification response. The Management Server must be capable of delivering ANPR reads to NAS within 2 seconds of capture.

For mobile ANPR systems the overall response time required is 6 seconds, with 2 seconds allocated to NAS to process the read and generate the hit notification response. The Management Server must be capable of delivering ANPR reads to NAS within 4 seconds of capture. Note: This requirement assumes that mobile units are connected. NASP provides separate timescales for mobile units that are not connected.

To maintain the throughput and required response times, new ANPR reads should be given priority over buffered data. The Management Server must be capable of ensuring a Last-In, First-Out approach is adopted for backlogged data.

The Management Server should allow administrators to identify issues with NRDs and to fault find by providing the capability to view the throughput of ANRP reads from individual cameras and to see camera connection status.

Reqt ID	Requirement
MS010	The Management Server shall deliver ANPR reads to NAS within 2 seconds of capture for static, moveable, dual lane and CCTV ANPR Integrated systems
MS011	The Management Server shall deliver ANPR reads to NAS within 4 seconds of capture for mobile ANPR systems
MS012	The Management Server shall transfer buffered data to the NAS in a Last-In-First Out queue
MS013	The Management Server shall provide the capability for LEAs to monitor camera throughput and connection

3.4 Resilience

The NAS solution has made provision for both resilience and disaster recovery. Where there is total loss of the primary site, the service will be made available from a standby data centre within 4 hours. To minimise the risk of end to end data loss, the Management Server shall be capable of buffering all ANPR reads and alarm responses. ANPR reads shall be stored by the Management Server for 7 days irrespective of whether the NAS has acknowledged receipt of the data. This is the maximum allowed by NASP. The Management Server must also provide indication to users of the state of the connection to NAS.

In the event of a failover being invoked and to ensure all data is received by NAS, the Management Server must be capable of re-sending the data sent to NAS in the 30 minutes leading up to the point where the connection was lost. This is in addition to the data buffered when the connection was not available. This additional 30 minutes of data should only be re-sent where connection to the NAS has been lost for a given period of time. This period should be configurable.

Reqt ID	Requirement
MS015	The Management Server shall buffer 7 consecutive days worth of ANPR reads irrespective of whether such data has been acknowledged as received by NAS
MS016	The Management Server shall be capable of resending buffered data
MS017	The Management Server shall clearly identify the state of connectivity to NAS and/or any time when data is not being sent to or received from NAS
MS018	The solution shall ensure that the Management Server can be returned to service within 72 hours of

	a loss of service in the event of failure.
MS019	The Management Server shall resend 30 minutes of ANPR read data for the period immediately before loss of connection to NAS.
MS020	The Management Server shall be capable of configuring the period of NAS connectivity loss before the additional 30 minutes of ANPR read data is re-sent.
MS021	The Management Server shall use DNS to resolve NAS addresses rather than using IP addresses

3.5 Data Exchange

The interface between the Management Servers and NAS is via a REST API developed by the NAS application supplier. The detailed definition for this can be found in the LPR Core REST API Document, ref [3] and the LPR Core API XML Specification, ref [4]. The Management Server shall use this interface for sending ANPR reads and alarm responses and for retrieving VOI lists, camera data and alerts.

NAS is capable of accepting updates to existing ANPR reads, providing all the meta data associated with the read is included. This is because NAS will replace the entire read originally received with the content of the re-submitted read. The functionality allows images to be submitted that were not available originally. The Management Server should aim to package messages to reduce the need to resend them. However, the delay should be no longer than 1 second to ensure that the required performance targets are still achieved.

NAS will only accept ANPR reads that contain a valid camera identifier. The Management Server must retrieve the master camera data from NAS and ensure that the latest version is maintained.

NAS allows VOI lists, updates to VOI lists and alerts to be retrieved for onward transmission to mobile units. The Management Server is responsible for retrieval of these items from NAS and for ensuring that that locally held data is kept up-to-date. This includes the deletion of VOI lists retrieve from NAS that have not been updated for more than 28 days. Where data is passed on to mobile units, the Management Server is responsible for the distribution of the data and ensuring that the data held by mobile units is kept up-to-date.

Reqt ID	Requirement
MS022	The Management Server shall utilise the NAS REST API to send and retrieve data
MS023	The Management Server shall package messages wherever possible to avoid the need to re-submit the read with more complete information.
MS024	The Management Server shall ensure that any re-submission of reads includes the full details including all the meta data.
MS025	The Management Server shall retrieve the master camera data from NAS in line with the API functionality
MS026	The Management Server shall ensure that locally held camera file data is up-to-date
MS027	The Management Server shall retrieve VOI lists and entries from NAS using the NAS API.
MS028	The Management Server shall be capable of maintaining up-to-date VOI lists
MS029	The Management Server shall ensure that NAS VOI lists held on the Management Server are the latest versions
MS030	The Management Server shall delete retrieved VOI lists after 28 days following the last update
MS031	The Management Server shall retrieve alerts from NAS using the NAS REST API
MS032	The Management Server shall manage the distribution of VOI lists to mobile units
MS033	The Management Server shall be capable of synchronising data for the VOI lists held by mobile units
MS034	The Management Server shall be capable of distributing alerts to mobile units
MS035	The Management Server shall enable users to append Additional Notes to the most recent VOI data in line with the API functionality
MS036	The Management Server shall enable users to submit a response to an alert in line with the API functionality
MS022	The Management Server shall utilise the NAS REST API to send and retrieve data

3.6 Identity and Access Management

Use of the Management Server and access to data must be controlled through a set of user permissions within the Management Server.

Reqt ID	Requirement
MS037	The Management Server shall facilitate the allocation of defined permissions to roles to restrict access to data, assets and functions.
MS038	The Management Server shall facilitate management of user roles which shows existing roles applied to each user and enables the allocation or removal of defined roles from each user.
MS039	The Management Server shall include provision for allocating different levels of audit roles. E.g. Some auditors cannot see some user activities.

3.7 Information Assurance

The Management Servers will communicate with NAS using the PSN Assured network. LEAs will be responsible for gaining accreditation for the connection of Management Servers to PSN. Communications between the NAS and the Management Servers will be protected from interception by the use of Transport Layer Security (TLS) to encrypt the data being transferred. The Management Server must ensure that older versions of TLS and Secure Sockets Layer (SSL) cannot be used.

The Management Server shall ensure that user actions are recorded and users are required to capture the reasons for accessing data. The records associated with this should be readily available to support audits.

Using Role Based Mandatory Access Control, NAS ensures that access to data is restricted. The Management Server shall ensure that the same controls can be applied for data that has been retrieved from NAS and is stored on the Management Server. Note: it is expected that business processes will need to be implemented to ensure that the same permissions are applied by administrators to both NAS and the Management Servers.

Reqt ID	Requirement
MS040	The Management Server shall communicate with NAS using the PSN Assured network.
MS041	The Management Server shall utilise TLS version 1.2 for all communications with NAS
MS042	The Management Server shall be configured to prevent use of older versions of TLS and SSL
MS043	The Management Server shall maintain easily accessible records for all significant actions on the system for audit purposes
MS044	The Management Server shall provide the capability for users to record the reasons for access to ANPR data for audit purposes
MS045	The Management Server shall ensure Role Based Mandatory Access Control is applied to all data downloaded from NAS, based on user identities, identification and authorisation, all managed by the Management Server independent of NAS

3.8 Transition to NAS

As part of the transition from NADC and BOFs to NAS and Management Servers, there will be a period where ANPR reads will be provided to both national systems. This dual running period is expected to be 3 months in duration. During this period, the BOFs will retain primacy of the read data, control of user accounts and the PNC interface. The solution will depend on the existing LEA infrastructure and the specific approach towards implementation of the Management Server and is therefore likely to be specific to each LEA.

Reqt ID	Requirement
MS046	The Management Server shall support the transition between NADC and NAS

4. Additional Guidance

The following subsections cover additional information that may be useful in the development of Management Server. The contents of this section are provided as guidance and therefore are not considered part of the formal requirements set. As such, the integration and connection tests will not exercise this functionality. However, LEAs may request the functionality is included in the scope of their solution and be tested accordingly. This will be down to individual LEAs. LEAs may wish to provide some degree of continuity through the form of local search capability in the event that the connections between the LEA infrastructure and NAS are lost. This functionality will be limited to full or partial VRM lookup using the data held on the Management Server.

Where this functionality is provided, the Management Server may also need to provide an alerting capability against locally held VOI lists, an alarm stack and the ability to correct misreads.

4.1 Integration with Local Infrastructure

The Management Server solution needs to integrate with a LEA's existing camera and mobile unit infrastructure. This may require the LEA to retain existing portals, especially where NRDs or mobile unit interfaces are proprietary.

For mobile units, there should be a mechanism that enables in-car users to be managed; ensuring that the data access restrictions in place in both NAS and the Management Servers is carried through to the in-car systems. The solution for achieving this will be heavily dependent of the type of in-car systems used.

Management Server suppliers will need to work with LEAs to understand the local infrastructure and provide any additional functionality to support it.